VTI Responses

UK Government Consultation:

Growing up in the online world

The following reflects the core portions of the VPN Trust Initiative's submission to the UK Government consultation *Growing up in the online world*.

VTI's comments focus specifically on areas where VPN providers and cybersecurity infrastructure operators have direct operational, technical, privacy, and cybersecurity expertise, particularly in relation to age assurance, circumvention, and proposals affecting VPNs and other privacy and security infrastructure.

Chapter 2: Interventions for safer, more positive experiences

Age of digital consent

Question

What risks or burdens may be associated with raising the minimum age of digital consent?

Response

Any increase in the minimum age of digital consent could create pressure for expanded age-verification obligations across a wider range of online services, including services fundamentally designed around privacy and security. Policymakers should carefully consider the operational, cybersecurity, and privacy implications associated with increased identity verification requirements and broader collection of sensitive personal information.

There is also a risk that broad or inconsistently applied obligations could unintentionally capture content-neutral infrastructure and security services whose primary purpose is not social interaction or content distribution.

Question

What should be considered to make raising the digital age of consent effective and workable?

Response

Any approach should be evidence-based, proportionate, technically feasible, and mindful of privacy and cybersecurity risks. Policymakers should distinguish between services that host or distribute content and general-purpose infrastructure or cybersecurity services.

Approaches requiring repeated age verification across many services may create substantial user friction while also increasing sensitive-data collection and expanding cybersecurity risks associated with storing or processing identity information.

Question

To what extent do you agree or disagree with the following statement:
“There is a case for changing the digital age of consent for some online services but not others”

Response

Somewhat agree.

Different categories of online services operate in fundamentally different ways and present different levels of risk. Policymakers should avoid applying identical obligations across services with widely different technical functions and societal purposes.

“Platform” is not a one-size-fits-all term. Services such as TikTok and Facebook are only one layer in a many-layered Internet. Content-neutral privacy and cybersecurity infrastructure services work at a more foundational layer, and should not automatically be treated the same way as social media or user-generated content platforms.

What services should age restrictions apply to

Question

What factors are important when determining which apps, sites or services to apply minimum age of access restrictions to?

Response

Different categories of online services operate in fundamentally different ways and present different levels of risk. Policymakers should avoid applying identical obligations across services with widely different technical functions and societal purposes. Policymakers should carefully distinguish between services that directly host, recommend, or distribute content and services functioning as general-purpose Internet infrastructure or cybersecurity tools.

Factors such as user-to-user interaction, content hosting, recommendation systems, and the nature of user engagement may be relevant considerations. However, content-neutral infrastructure services whose primary purpose is privacy, security, or network access should be treated differently from content or platform-layer services.

Question

Are there any types of apps, sites or services that you want to be captured by minimum age of access restrictions?

Response

VTI's primary concern is ensuring that content-neutral privacy and cybersecurity services are not unintentionally swept into regulatory frameworks designed for social or content platforms.

Question

What factors are important when determining which apps, sites or services to apply age restrictions on specific features and functionalities?

Response

Any restrictions should be evidence-based, proportionate, technically feasible, and targeted toward the services directly responsible for the relevant user interaction or content experience.

Policymakers should also consider whether proposed measures can realistically achieve their stated goals without creating unintended privacy, cybersecurity, or operational consequences.

Question

Are there additional types of service which you think would be appropriate to exempt from age restrictions?

Response

Yes. Policymakers should carefully consider exemptions for services whose primary purpose is cybersecurity, privacy protection, enterprise security, educational access, or network infrastructure.

This may include VPN services and other content-neutral technologies designed primarily to protect users and secure communications.

Chapter 3: Enforcement and compliance

Age assurance

Question

To what extent do you agree or disagree with the following statement:
“Adults should complete age checks more often, if it means children are safer online”?

Response

Neither agree nor disagree.

Question

What should be considered to make minimum age restrictions effective and workable?

Response

Approaches should remain proportionate, evidence-based, privacy-preserving, technically feasible, and focused on minimizing unnecessary collection of sensitive personal information.

Policymakers should also carefully distinguish between services directly responsible for hosting or distributing content and general-purpose infrastructure or cybersecurity services which are content neutral.

Question

What do you think the impacts might be from requiring age assurance across a greater number of online platforms?

Response

Broad expansion of age assurance requirements may significantly increase sensitive-data collection across the online ecosystem while also creating additional cybersecurity, operational, and privacy risks.

Repeated identity-verification requirements may reduce user trust, increase friction for legitimate users, and create additional incentives for the collection and retention of sensitive personal information.

Question

How, if at all, could age assurance be made more effective?

Response

Approaches should prioritize proportionality, interoperability, minimization of repeated verification requests, and strong privacy protections.

Measures are most likely to be effective when they remain focused on services directly responsible for content or user interactions rather than extending obligations to general-purpose infrastructure.

Question

What should be considered when assessing the effectiveness of age-verification and age-assurance technologies?

Response

Assessment should consider not only accuracy, but also privacy implications, cybersecurity risks, accessibility, user trust, technical feasibility, and the potential for circumvention or overblocking.

Circumvention of age limits

Question

What methods to circumvent online safety rules do you think children in the UK use, beyond VPNs, or similar technologies?

Response

The premise of the question is somewhat flawed in that it presumes that children use VPNs to circumvent online safety rules. The available evidence demonstrates that children use VPNs for the same reasons adults do: namely, to enhance privacy and security and to avoid online harms such as cyber crime, profiling, discrimination, censorship, and throttling. There is limited evidence that children use VPNs to circumvent online safety rules, particularly as to reputable paid VPN services which require payment methods.

Potential methods to access restricted content may include the use of shared accounts, inaccurate identity information, browser-based tools, alternative DNS configurations, proxies, remote-access tools, or assistance from peers or adults.

More broadly, policymakers should recognize that circumvention challenges are not unique to VPNs and often reflect broader limitations associated with age-assurance systems themselves. Applying age-assurance at the content level—social media, user-generated content, and video-sharing platforms—would be more targeted and effective than applying age-assurance at infrastructure services because this is where content is actually made available, and these services already hold user-related information that can inform decisions about age-appropriate experiences.

If the scope of services subject to age verification were nonetheless considered for expansion, a single, centralised mechanism at the services distribution layer, such as app stores, would be the most proportionate approach, enabling age assurance to occur once rather than being replicated across individual services.

Question

Which option should the government prioritise to reduce circumvention of online safety rules in the UK?

Response

More education for children.

Digital literacy, online safety education, and support for families are likely to be more sustainable and effective approaches than attempting to regulate general-purpose cybersecurity tools relied upon by millions of legitimate users.

Question

To what extent do you agree or disagree with the following statement:
"Everyone should go through age checks to access a VPN if it would prevent children using them"

Response

Strongly disagree.

The very structure of this question would seem to signal a misunderstanding of the issue, since "preventing young people from using VPNs" is not the same thing as "keeping children safe from online harms." By preventing users from using a VPN we could be exposing those users to more online risks because they would be deprived of a cybersecurity tool that protects their data and privacy when navigating online.

Question

What do you think the impacts would be if VPNs were age-restricted?

Response

VPNs are widely used cybersecurity and privacy tools relied upon by businesses, schools, journalists, healthcare providers, government officials, families, and ordinary users.

Age-restricting VPNs could risk degrading the privacy-preserving nature of these services by introducing identity-verification and additional data-collection requirements into systems intentionally designed to minimize the collection of personal information. This would create a regime that makes access to basic privacy tools conditional on disclosing further sensitive information for all users, including adults. Many adults have legitimate concerns about sharing sensitive personal data online, particularly given the increasing frequency of hacking incidents and data breaches, and those concerns are especially prevalent amongst more vulnerable individuals, such as activists, journalists and human rights defenders.

Restricting reputable VPN providers may also produce unintended user-safety consequences. Users seeking privacy protections could migrate toward less trustworthy or unregulated services that rely on aggressive data collection, deceptive practices, or weak security protections, or stop

using VPN services altogether. This would reduce overall cybersecurity and safety online for all users, including minors.

Available research currently suggests there is limited evidence that children are using VPNs at scale to bypass age restrictions. Efforts to enforce age restrictions at the infrastructure layer would therefore risk significant overblocking, reduced service availability, or market withdrawal by some providers.

Policymaking in this area should remain evidence-based, proportionate, and focused on measures capable of achieving meaningful child-safety outcomes without undermining or discouraging widely used cybersecurity tools.

Question

What should be considered to make age-restricting VPNs effective and workable?

Response

Policymakers should carefully consider whether such measures are technically feasible at all without undermining privacy, cybersecurity, and legitimate use cases.

Determined users would likely continue to circumvent restrictions using a variety of other readily available tools and technologies, potentially pushing users towards less trustworthy operators.

Policymakers should also consider the larger societal role VPNs play in protecting everyone's sensitive communications, securing remote work and education, safeguarding vulnerable users, and supporting cybersecurity resilience more broadly.

VTI will continue supporting research efforts to improve the evidence base around VPN use and circumvention behaviours so future policymaking can remain evidence-based and proportionate.